작성자:
Pedro Palandrani
리서치 애널리스트

날짜: 2020년 4월
15일 주제: 테마

Global X ETF 리서치

# 사이버 보안은 사물인터넷 성장을 어떻게 가속화시키는가

2020년대는 어디에서나 연결이 가능한 스마트 시대로 정의될 수 있습니다. 가정, 직장 및 도시에서 모든 유형의 스마트기기가 인터넷으로 연결되어 순조롭게 데이터를 포착하고 전송할 수 있습니다. 지난 10년 동안 반도체 원가는 90% 이상 낮아져 이러한 스마트기기들이 상용화 되었습니다. 5G 개시와 더불어 데이터는 4G보다 최대 100배 빠르게 스마트기기와 클라우드 간에 거의 즉각적으로 전송됩니다.

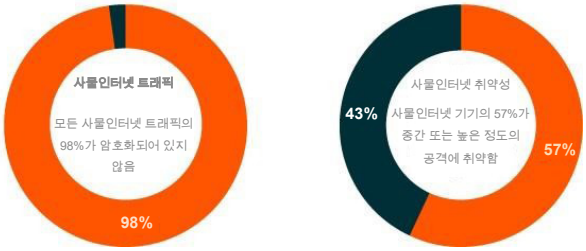
사물인터넷을 통해 수백만 개의 기기가 온라인으로 연결됨에 따라 개인과 기업에게는 엄청난 기회가 생길 뿐 아니라 새로운 유형의 위험 및 취약점도 생깁니다. 이러한 수백만 개의 기기는 해커들에게는 새로운 진입점으로 작용하여 회사와 개인 입장에서 보안을 효과적으로 관리하기가 어려워지고 복잡해졌습니다. 사물인터넷을 성공적으로 배치하기 위해서는 사전에 보안 요건을 세우는 것에서부터 기계가 산출하는 데이터의 지속적인 관리 및 보호에 이르기까지 여러 겹으로 이루어진 종단간 보안이 요구됩니다.[1] 만능 솔루션은 없지만 세계의 선도적인 사이버 보안 회사들은 새로운 인터넷 시대에 이렇듯 거대한 확장을 보호하기 위해 준비하고 있는 중입니다.

## 새로운 기기, 새로운 위협

사물인터넷은 자율주행차, 스마트 도시, 스마트 공장 및 건강관리 기기를 포함해 많은 신흥 기술과 테마에 있어서 매우 중요합니다. 그러나 인터넷을 이용하는 기기는 소중한 개인 데이터를 훔치거나 그 대가를 요구하는 해커들에게는 새로운 타겟이 되기도 합니다. 오늘날, 사물인터넷 트래픽의 98%가 암호화되어 있지 않아 사물인터넷 기기의 57%가 사이버 공격에 매우 취약하고 네트워크 상에서 개인 데이터 및 기밀 데이터를 위험에 빠뜨립니다.[2] 커넥티드 기기가 많아짐에 따라 사고의 건수와 정도도 증가하리라 예상할 수 있습니다.

**사물인터넷의 사이버 보안**

출처: Palo Alto Networks

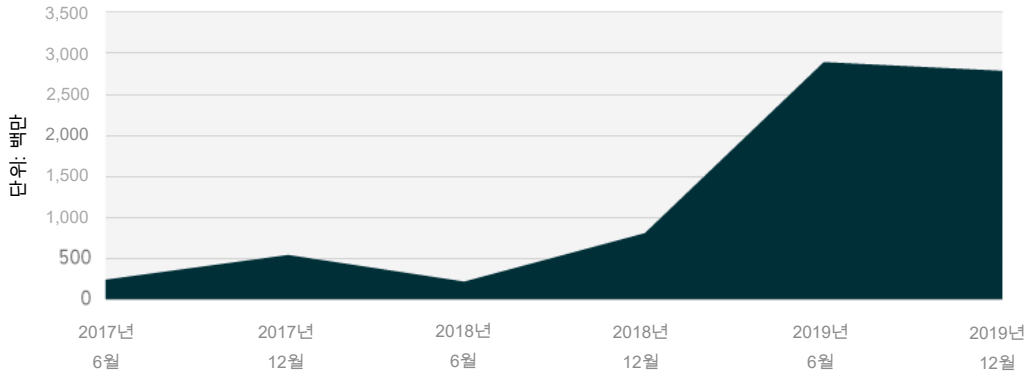



가상의 비서를 통해 우리 가정에 진입하려는 인터넷 자이언트에서부터 자라난, 비교적 새로운 시장인 스마트 스피커를 예로 들어보겠습니다. 2018년 해커들은 아마존의 Alexa 코드의 취약성을 틈타 사용자들을 엿들을 수 있었습니다. 본래 Alexa는 “Alexa”라는 웨이크워드를 탐지한 후에 녹음을 시작하고 “Turn off the lights(조명을 꺼)!”라는 명령어를 들은 후에 녹음을 종료합니다. 하지만 해커들은 Alexa가 명령어를 들은 후에도 한참 동안 계속해서 녹음을 하도록 프로그램을 짜 사용자의 대화를 녹음할 수 있었습니다. 다행히도 해커들은 실제로 악의가 없는 연구원들이어서 그들이 발견한 내용을 아마존에 경고하였습니다.[3] 아마존은 즉시 보안을 수정했습니다.

하지만 악의를 가진 해커들이 많고 그러한 해커들은 늘어나고 있습니다. 방어 계획을 짜도록 돕기 위해 사이버 보안 회사들은 허니팟을 유인 서버로 사용하여 사이버 공격의 동향과 패턴을 측정합니다. 전 세계에 설치된 허니팟은 멀웨어에 감염된 스마트워치나 커넥티드 칫솔과 같은 커넥티드 기기로부터 공격을 받을 수 있습니다. 2019년, 보안 연구가들은 허니팟이 공격 트래픽이 전년 대비 446% 증가했다고 기록한 사실을 발견했습니다(공격 수가 10억 건에서 57억 건으로 증가).[4]

## 기간별 글로벌 총 허니팟 공격

출처: F-Secure, 공격 일람 2019년 하반기




참고: 추정치에 전통적인 커넥티드 기기가 포함됨

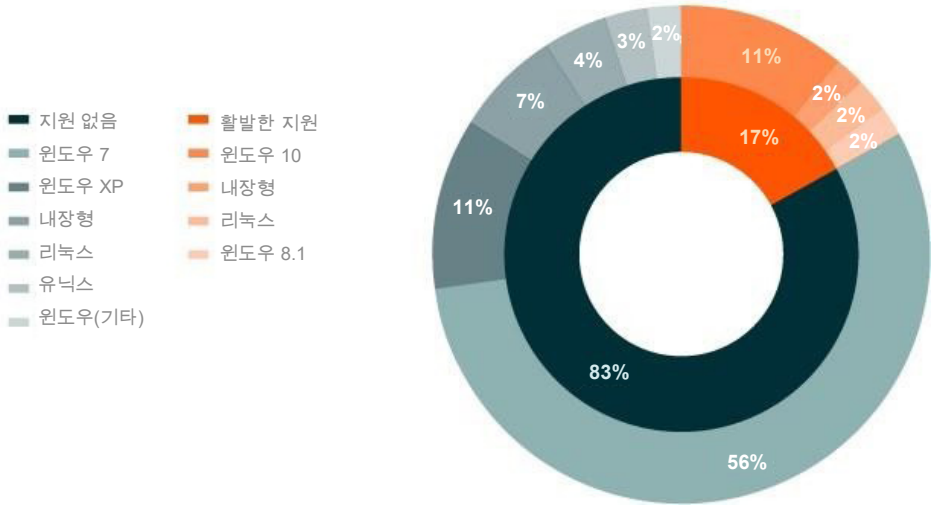
## 건강도 해킹을 당할 수 있습니다

커넥티드 카, 스마트 도시 및 차세대 건강 기기의 출현으로 인해 해커들은 가상 세계에서 사적인 데이터를 훔칠 수 있을 뿐만 아니라 가상의 세계와 실제 세계를 연결하는 기기를 타겟으로 할 수 있습니다. 의료용 사물인터넷(IoMT)을 구성하는 기기는 해커들에게 특히 민감한 진입점입니다. 2013년, 해킹 공포로 인해 전임 미국 부통령 딕 체니는 와이파이로 연결된 심박조율기를 와이파이가 없는 것으로 교체해야 했습니다.[5] 4년 후, 미국 식품의약국(FDA)은 해킹 가능성 때문에 거의 50만 개의 커넥티드 심박조율기를 회수했습니다.[6] 디지털 알약은 또 하나의 잠재적인 타겟입니다. 디지털 알약은 위장관을 따라 내려가면서 진단 정보를 파악할 수 있는 칩이 있어서 해커들이 그러한 정보를 가로챌 수 있습니다.[7]

사물인터넷 영상 기기에 대한 최근의 연구에 의하면 83%가 지원을 받지 않는 운영 시스템 상에서 진행되고 있습니다.[8] 이러한 기기를 사용하는 의료조직은 민감한 의료 정보를 노출시킬 수 있는 공격에 점점 더 취약해질 가능성이 있습니다.

## 의료 영상 기기에 대한 운영체제 지원 내역

출처: Palo Alto Networks. 2019년 12월 31일 기준.




이와 같은 커넥티드 기기의 안전을 지키는 방법에 답하는 것은 의료서비스 제공자와 환자가 이러한 기술을 안전하게 사용하는 것이 가장 중요합니다. 의료용 사물인터넷 제조사에는 특히나 중요합니다. FDA 지침에 따라 제조사는 안전성 및 성능에 대해 전적인 책임을 집니다.[9]

### 엔드포인트 안전 확보

초기의 엔드포인트 보안 회사들은 노트북, PC 및 스마트폰에 중점을 두었지만 이제는 종종 커넥티드 사물인터넷 기기에도 활용되고 있습니다. 엔드포인트는 두 개의 주요 카테고리로 구성되어 있습니다. 사용자 상호작용 포인트에는 스마트폰과 같이 사용자가 명령어를 입력하고 사용자의 기기가 요청한 정보를 표시하는 기기, 두 번째 카테고리에는 스마트 스피커 또는 스마트 전구와 같이 사용자의 명령에 반응하는 작동기 또는 센서 기기가 포함됩니다.

## 사물인터넷 생태계의 인프라

출처: Nan Zhang, Soteris Demetriou 외 Data Crystal Ball을 통한 사물인터넷 보안 이해: 우리는 지금 어디에 있으며 어디로 가고 있는가


사물인터넷 아키텍쳐는 일반적으로 양방향이어서 데이터가 작동기 또는 센서에서 생성되어 사용자 상호작용 포인트와 클라우드 저장소 모두로 보내집니다. 예를 들면, 스마트 보안 카메라는 움직임을 감지하여 전화기로 통지를 보내고 이미지를 클라우드에 저장합니다.

이러한 아키텍쳐에서 사물인터넷 기기, 사용자 상호작용 포인트 및 클라우드 저장소는 데이터를 보호하기 위한 보안 조치가 필요합니다. 사물인터넷 기기에는 하드웨어에 패치된, 마이크로코드라고도 불리는 운영 소프트웨어 내 보호장치가 있어야 합니다. 따라서 오늘날의 사이버 보안 회사들은 사물인터넷 기기 제조사와 기기 디자인 및 테스트, 사고 대응, 처리 모델링에서 서로 협력합니다.[10]

네트워크에 대한 접근 통제 역시 매우 중요하여 네트워크 방화벽 회사가 역할을 맡고 있습니다. 이러한 회사들은 네트워크에 있는 모든 기기를 식별하고 프로필을 만듭니다. 그들은 기기를 지속적으로 모니터링하여 기기가 침해되지 않도록 하며, 침해된 경우에는 즉각적인 조치를 취합니다.[11]

## 싸움 중인 AI

사이버 보안 회사 및 기기 제조사는 인공지능(AI) 및 머신 러닝(ML) 애플리케이션을 점점 더 많이 사용하여 맞춤형 엔드포인트 보안 솔루션을 제공하고 있습니다. 사물인터넷 기기는 그 수와 종류가 너무도 다양하므로 인공지능은 확장성이 있는 맞춤형 사이버 보안 시스템을 제공하는 데 도움이 됩니다. 그러한 알고리즘은 하드코드화된 속성과 행동에 기초하여 기기를 식별하도록 훈련을 받습니다. 또한 네트워크에 설치된 알고리즘은 감지 엔진을 사용하여 자율적으로 이러한 기기의 '정상' 행동을 배울 수 있습니다. 예를 들자면, 심박조율기 또는 스마트 알약에서 인공지능은 이전의 결과에 근거하여 성능을 예측하고 기기가 비정상적으로 작동한 시점을 알아낼 수 있습니다. 행동에 변화가 생기는 경우 그것은 기기에 문제가 생겼거나 공격을 받았다는 잠재적인 신호일 수 있습니다.

사이버 보안 방어용으로 인공지능이 사용되지만 해커들 역시 인공지능을 이용하여 데이터 오염과 같이 새롭고 정교한 사이버 위협을 만들고 있습니다. 향후 2년 동안 모든 인공지능 사이버 공격의 30%가 교육용 데이터 오염으로 활용될 것으로 예상됩니다.[12] 데이터 오염은 침해된 그리고 악성인 데이터를 사물인터넷 또는 커넥티드 기기에 입력하여 시스템이 데이터를 잘못 분류하게 만듭니다. 새로운 인공지능 기반 사이버 공격을 막기 위해 사이버 보안 회사들은 계속 자사의 인공지능 애플리케이션을 강화합니다.

## 결론

커넥티드 기기의 지속적인 물결 속에서 만능 사이버 보안 솔루션은 없습니다. 그러나 세계의 선도적인 사이버 보안 회사와 사물인터넷 제조사들은 계속 그들의 전략을 개선하고 최근 기술을 활용하여 보호 조치를 실시합니다. 사물인터넷이 인프라, 건강관리 및 운송과 같은 새로운 길로 계속 확장하므로, 사이버 보안 회사들은 이러한 기기를 안전하게 하는 데 중심 역할을 수행하여 디지털 공격이 실제 피해로 이어지지 않도록 하는 것이 매우 중요합니다.

작성자:

각주

1. IoT Cybersecurity Alliance, “사물인터넷 사이버 보안 이해”, 2017년.
2. Palo Alto Networks, “2020년 유닛 42 사물인터넷 위협 보고서”, 2020년 3월 10일.
3. Wired, “해커, Amazon Echo를 스파이 버그로 만드는 (그리 쉽지 않은) 방법을 발견하다”, 2018년 8월 12일.
4. F-Secure, “공격 일람 2019년 하반기: 사이버 공격에 있어 선례가 없는 해”, 2020년 4월 3일.
5. Forbes, “신체인터넷이란 무엇인가? 그리고 그것이 세계를 어떻게 변화시키고 있는가?”, 2019년 12월 6일
6. Business Insider, “FDA, 해킹에 대한 두려움 때문에 약 50만 개의 인터넷에 연결된 심박조율기를 리콜하다”, 2017년 9월 1일.
7. Alliance of Advanced BioMedical Engineering, “스마트 알약으로 진단이 편리해지고 치료가 정확해지다”, 2017년.
8. Palo Alto Networks, (n2).
9. FDA, “FDA가 환자, 서비스 제공자 및 제조사에 특정 커뮤니케이션 소프트웨어를 사용하는 커넥티드 의료 기기 및 건강관리 네트워크의 잠재적인 사이버 보안 취약성에 대해 알리다”, 2019년 10월 1일.
10. Rapid 7, “사물인터넷 보안 테스트 서비스”, 2020년 3월 31일에 접속.
11. Fortinet, “사물인터넷이 배치된 네트워크 보호”, 2020년 3월 31일 접속.
12. Business Chief, “Gartner: 10대 기술 추세”, 2020년 3월 11일

투자에는 원금 손실 가능성을 포함한 리스크가 수반됩니다. 국제 투자에는 통화 가치의 불리한 변동, 일반회계원칙의 차이, 또는 다른 국가의 경제적 또는 정치적 불안정으로 인해 자본 손실을 입을 위험이 수반됩니다. 신흥시장에는 동일한 요인뿐만 아니라 변동성의 증가 및 낮은 거래량과 관련된 고도의 리스크가 수반됩니다.
단일 국가에 초점을 맞춘 증권 및 좁은 시각으로 본 투자는 변동성이 높아질 가능성이 있습니다.